IN THE SPECIFICATION

Please amend paragraph 10 beginning on page 6 as follows:

The authentication server 106 provides authentication service by performing registration methods, such as the ones shown in Figures 8 and 9 and by performing authentication and authorization methods, such as the ones shown in Figures 5-7 and 10. Registration is the process of associating authentication verification information with an individual identity. Authentication is the process of authenticating a user 102 and associating a level of assurance with the authentication of the user 102. Authorization is the process of deciding whether to grant a request to a user 102 based on the request of the user 102, the ~~permissions of the user 102~~ permission of the relying party 104, and the level of assurance provided by the authentication. Registration, authentication, and authorization may all be performed by one server, as shown in Figure 1, or divided among a number of servers. For example, Figure 4 shows a registration server, an authentication server, and an authorization server.

Please amend paragraph 11 beginning on page 6 as follows:

Consider a user 102 who wants to buy an item in a store using a credit card. The store is a relying party 104 using an authentication service to process the credit card transaction. To get a credit card, a user 102 first fills out a form applying for it. The credit card company takes the information from the form and processes it to decide whether to open an account for the user 102. That is [[like]] similar to registration. After the credit card is sent to the user 102,

the user 102 presents the card in the store to buy something. The store clerk requests authentication by asking for a picture ID and comparing the signature on the back of the card to the user's 102 signature. This is similar to authentication. The clerk runs the card through a machine to see if the purchase is approved by the credit card company or not. The credit card company may check if the user's 102 credit limit is exceeded. This is [[like the]] similar to authorization. If the purchase is approved, the transaction is completed. This is analogous to access being granted. Embodiments of the present invention provide a system to similarly authenticate a user 102 for an online transaction.

Please amend paragraph 35 beginning on page 19 as follows:

When a user 302 authenticates himself, the authorization [[sever]] server 306 specifies the level of assurance in the authentication required for the requested transaction with the relying party 304. The authorization server 306 optionally specifies the function for the authentication server 308 to use to compute the level of assurance. If the user 302 does not meet the level of assurance, then the authentication server 308 requests that the user 302 use an additional authentication mechanism. If the user 302 successfully completes the authentication, then the authentication server 308 reports the identity of the user 302 and the level of assurance to the authorization service 306. The authorization server 306 determines if that user 302 is authorized for the requested transaction with the given level of authentication. If so, the user's 306 request is fulfilled. Otherwise, it is denied.

Please amend paragraph 43 beginning on page 23 as follows:

In addition to having different levels of authentication, there are optionally different levels of identity confirmation. ~~For example~~ For example, there might be four levels of identity confirmation associated with the AMA web site as follows: level 1 (a student Internet ID), level 2 (a professional Internet ID), level 3 (a confirmed Internet ID), and level 4 (a notarized Internet ID). The level 1 confirmation level is for medical students who are attending an accredited U.S. medical school. A student Internet ID is issued online at the AMA web site. Once the AMA receives a graduation report and/or medical licensure, the student can terminate [[this]] his or her student Internet ID, and apply for a professional Internet ID. The level 2 confirmation level is available to all physicians. A professional Internet ID is issued online at the AMA web site. Physicians input their name, state, zip code, data of birth, social security number, Drug Enforcement Administration (DEA) number, last year of residency, medical license number and state. This information is matched against an AMA physician masterfile. The level 3 confirmation level is an upgrade from level 2. Confirmation for the upgrade takes place over the phone or through the U.S. mail, after a physician requested the upgrade at the AMA web site and entered the zip code for his practice. He enters the address of his practice and the AMA confirms the address and sends a confirmation code to the physician by U.S. mail. The physician then returns to the AMA web site and enters the confirmation code to upgrade. The level 4 confirmation level is an upgrade from level 3. At the AMA web site, a physician selects the upgrade, which generates a printout that includes

authentication verification information provided by the physician such as the hash of the physician's public key. The physician has the form notarized and mails it to the AMA. After the form is received and confirmed, the AMA approves the upgrade.

Please amend paragraph 44 beginning on page 23 as follows:

Embodiments of the present invention provide an extensible system to authenticate users in real time wherever they are and with whatever authentication devices are currently available to them. ~~[0045]~~ In another embodiment of the method 500, at least one of the authentication mechanisms is mobile.

Please amend paragraph 62 beginning on page 32 as follows:

Figure 10 is a flow chart that shows an embodiment of a method of authentication 1000 for systems such as the ones shown in Figures 1-4.40. One aspect of the present invention is a method of authentication 1000. The method 1000 comprises a user requesting a protected service from a relying party 1002. ~~The relying~~ The relying party sends a description of the request to an authorization server 1004. The authorization server determines a first level of assurance and sends the first level of assurance to an authentication server 1006. The authentication server requests authentication from the user 1008. The user enters authentication information into an authentication device 1010. The authentication device sends authentication information to the authentication server 1012. The authentication server verifies the authentication information using authentication verification information stored in a portfolio in a database that is associated with the

user 1014. The authentication server computes a second level of assurance 1016. The second level of assurance is evaluated to see if it is high enough 1018. Upon determining the second level of assurance is high enough, the authentication server sends a first success message to the authorization server 1020. The authorization server verifies information from the authentication server and verifies that the user is allowed to perform the protected service and then sends a second success message to the relying party 1022. Upon verification of the information from the authentication server and verification that the user is allowed to perform the protected service, the relying party provides the protected service to the user 1024.